UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/600,113	06/20/2003	Amit Raikar	200309309-1	7736

22879 7590 02/11/2009

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
CERVETTI, DAVID GARCIA	
ART UNIT	**PAPER NUMBER**
2436	

NOTIFICATION DATE	DELIVERY MODE
02/11/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/600,113	RAIKAR ET AL.	
	Examiner	Art Unit	
	David García Cervetti	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 November 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 April 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's arguments and appeal brief filed November 17, 2008, have been fully considered.

2. Claims 1-16 are pending and have been examined. Claims 17-20 have been canceled.

Response to Amendment

3. Applicant's arguments with respect to the prior art have been considered but are moot in view of the new ground(s) of rejection.

4. In view of the appeal brief filed on November 17, 2008, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

5. To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

6. A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below: /Nasser G Moazzami/ Supervisory Patent Examiner, Art Unit 2436

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier et al. (US Patent Application Publication 2002/0087882, hereinafter Schneier), and further in view of Yoon et al. (US 7,386,733, hereinafter Yoon).

Regarding claims 1 and 8, Schneier teaches

an integrated intrusion detection method comprising (par. 37):

gathering information from a plurality of different types of intrusion detection sensors (pars. 35-36, monitors and collects information from sensors);

processing said information, wherein said processing provides a consolidated correlation of said information (pars. 64-65, analysis);

assigning a response corresponding to said information (pars. 87-88, determine response) and corresponding to said severity (par. 88-94, incidents have severity levels and responses correspond to severity levels); and

implementing said response (pars. 87-88, initiates response) according to said severity (par. 88-94, incidents have severity levels and responses correspond to severity levels).

Schneier does not expressly disclose, however, Yoon teaches assigning a severity to said information based on an enterprise wide security policy (col.6, lines 1-25, policies apply to intrusion information and alert messages).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to apply security policies to the IDS information of Schneier as taught by Yoon. One of ordinary skill in the art would have been motivated to perform such a modification to provide a policy based intrusion detection and response system (Yoon, col.3-4).

Regarding claims 2 and 9, the combination of Schneier and Yoon teaches wherein said information includes intrusion detection alerts (Schneier, pars. 62-64, alerts).

Regarding claim 3, the combination of Schneier and Yoon teaches centrally tracking information associated with intrusion detection alerts from said plurality of different types of intrusion detection sensors (Schneier, pars. 35-36, monitors and collects information from sensors, pars. 63-64).

Regarding claim 4, the combination of Schneier and Yoon teaches wherein said tracking information associated with intrusion detection includes assigning severity assignments standardized across said plurality of different types of intrusion detection sensors (Schneier, pars. 21 and 42, prioritize, par. 105, modify priority of problem).

Regarding claim 5, the combination of Schneier and Yoon teaches wherein said intrusion detection alerts are correlated based upon various alert attributes (Schneier, pars. 88-94, alerts and links to possible responses).

Regarding claim 6, the combination of Schneier and Yoon teaches wherein said response conforms to an enterprise wide strategy (Schneier, par. 60, rules).

Regarding claim 7, the combination of Schneier and Yoon teaches managing said intrusion detection sensors (Schneier, par. 37, adaptive sensors, receive updates dynamically).

Regarding claim 10, the combination of Schneier and Yoon teaches wherein said integration module selects appropriate hooks in an intrusion detection system (Schneier, pars. 41-42, connecting through pipes).

Regarding claim 11, the combination of Schneier and Yoon teaches wherein said data collection module logs alerts from said plurality of different types of intrusion detection sensors (Schneier, pars. 35-36, monitors and collects information from sensors, pars. 63-64).

Regarding claim 12, the combination of Schneier and Yoon teaches wherein said alerts are provided by a simple network management protocol (SNMP), a system log and an application program interface (Schneier, par. 36, SNMP sensors, syslogs, SNMP traps).

Regarding claim 13, the combination of Schneier and Yoon teaches wherein said integration module includes analyzing a plurality of manners in which an alert can be provided and selecting the manner that is the most secure with the least dependencies in a communication path (Schneier, pars. 63, selecting alert method).

Regarding claim 14, the combination of Schneier and Yoon teaches wherein said integration module utilizes a network application management platform to log information (Schneier, pars. 58-60, SOCRATES).

Regarding claim 15, the combination of Schneier and Yoon teaches wherein: an open view operation simple network management protocol trap is utilized to handle simple network management protocol trap based alerts; an open view operation log file encapsulator handles system log based alerts; and an open view message interceptor handles application program interface propagated alerts with the help of an operation message mechanism (Schneier, par. 36, SNMP sensors, syslogs, SNMP traps).

Regarding claim 16, the combination of Schneier and Yoon teaches wherein a secure open view template configuration is utilized to log information and the one message group is configured for handling intrusion detection system alerts and another message group is configured for handling intrusion detection system errors (Schneier, pars. 106-108, diverse groups and individuals are configured to receive alerts).

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David García Cervetti whose telephone number is (571)272-5861. The examiner can normally be reached on Monday-Tuesday and Thursday-Friday.

10. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

11. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David García Cervetti/
Primary Examiner, Art Unit 2436

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436